



UNITED STATES PATENT AND TRADEMARK OFFICE

A
UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/817,812	03/26/2001	John R. Douceur	MS1-734US	7817
22801	7590	07/14/2005	EXAMINER	
LEE & HAYES PLLC 421 W RIVERSIDE AVENUE SUITE 500 SPOKANE, WA 99201			FIELDS, COURTNEY D	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 07/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/817,812	DOUCEUR ET AL.	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 21 April 2005.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-44 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) 29-36 is/are allowed.
- 6) Claim(s) 1-28 and 37-44 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>02/22/05, 05/09/05</u>	6) <input type="checkbox"/> Other: _____

DETAILED ACTION

1. Claims 1-44 are pending.

Information Disclosure Statement

2. The Information Disclosure Statements respectfully submitted on 22 February 2005 and 09 May 2005 have been considered by the Examiner.

Allowable Subject Matter

3. Claims 29-36 are allowed.

Response to Arguments

4. Applicant's arguments filed 21 April 2005 have been fully considered but they are not persuasive.

5. Regarding claims 1 and 14, the Applicant argues that prior art Etzel et al. does not teach nor disclose performing a check whether a mapping of the access control entry to the symmetric key exists in an encrypted key cache and if the mapping exists, use the mapped symmetric key from the encrypted key cache to decrypt the file otherwise decrypt the encrypted symmetric key and use the decrypted symmetric key to decrypt the file. The Examiner respectfully disagrees and contends that Etzel et al. does teach a mapping of an access control entry to a symmetric key by using a ACS. The ACS maintains a database of symmetric keys so that shared keys may be accessed by the user. (See Column 6, lines 23-25) The symmetric key is known as the CV key. A copy of the CV key is encrypted and stored within a key cache memory. The symmetric key (CV key) is shared among the terminals and used to decrypt encrypted video program (file). Otherwise, the processor can also unload the encrypted program

encryption key used to encrypted the requested program video program from its database and use a local key to decrypt the encrypted program encryption key. (See Column 7, lines 7-19)

6. Regarding claims 5 and 18, the Applicant argues that the prior art Etzel et al. does not teach nor disclose generating a file including a key cache, encrypting the generated file using the private key and storing the encrypted file. The Examiner respectfully disagrees and contends that Etzel et al. does teach a DES processor having access to an encrypted key cache by obtaining a key from the key cache to encrypt incoming data that is received and store the data within the key cache by using a memory location address. (See Column 9, lines 34-50)

7. Regarding claims 7 and 20, the Applicant argues that the prior art Etzel et al. does not teach nor disclose obtaining an encrypted key cache, in encrypted form, from a remote storage device, to decrypt the key cache and use the key cache. The Examiner respectfully disagrees and contends that Etzel et al. does teach obtaining an encrypted key cache using a security module. The security module stores the encryption CV key that it shares with the ACS and the decrypted shared key. The stored decrypted program key in the key cache memory is used to decrypt the associated encrypted program when received by the server. (See Column 7, lines 37-45)

8. Therefore the rejection of claims 1-28 and 37-44 are maintained in view of the reasons above and below.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-28 and 37-44 are rejected under 35 U.S.C. 102(e) as being anticipated by Etzel et al. (U.S. Patent No. 6, 577, 734). Referring to the rejection of claims 1 and 14, Etzel et al. discloses a method, system, and computer-readable media receiving an access control entry corresponding to a file and including a symmetric key encrypted with a public key, checking whether an access control entry to symmetric key mapping exists in a key cache, and obtaining the symmetric key from the key cache if the mapping exists otherwise decrypting the encrypted symmetric key using a private key corresponding to the public key in Column 7, lines 7-45.

Referring to the rejection of claims 2 and 15, Etzel et al. discloses the claimed limitation wherein the public key and the private key are both part of a public/private key pair associated with a user in Column 4, lines 35-42.

Referring to the rejection of claims 3 and 16, Etzel et al. discloses the claimed limitation wherein receiving an access control list including a plurality of access control entries, selecting one of the plurality of access control entries that corresponds to the user, and

Art Unit: 2137

using at the access control entry, the selected one of the plurality of access control entries in Column 6, lines 23-46.

Referring to the rejection of claims 4 and 17, Etzel et al. discloses the claimed limitation wherein if the mapping does not exist, then creating, after decrypting the encrypted symmetric key, a new mapping in the key cache that maps the access control entry to the symmetric key in Column 6, lines 23-42.

Referring to the rejection of claims 5 and 18, Etzel et al. discloses the claimed limitation wherein generating a file including a key cache, encrypting the generated file using the private key and storing the encrypted file in Column 7, lines 9-16.

Referring to the rejection of claims 6 and 19, Etzel et al. discloses the claimed limitation wherein generating a file including the key cache, encrypting the generated file with another symmetric key, generating a new access control entry corresponding to the generated file, encrypting the other symmetric key with the public key and storing both the encrypted other symmetric key and an identifier of a user corresponding to the key cache in the new access control entry in Column 8, lines 5-26.

Referring to the rejection of claims 7 and 20, Etzel et al. discloses the claimed limitation wherein obtaining a key cache in encrypted form from a remote storage device, decrypting the key cache using the private key, and using as the key cache the decrypted key cache in Column 5, lines 35-66.

Referring to the rejection of claims 8, 21, and 25, Etzel et al. discloses the claimed limitation wherein decrypting using the private key, a symmetric key corresponding to

the key cache, and decrypting, using the symmetric key corresponding to the key cache, the key cache in Column 4, lines 9-19.

Referring to the rejection of claims 9 and 22, Etzel et al. discloses the claimed limitation wherein the checking comprises indexing into the key cache based on the encrypted symmetric key of the access control entry in Column 5, lines 20-34.

Referring to the rejection of claims 10 and 23, Etzel et al. discloses the claimed limitation wherein the checking comprises indexing into the encrypted key cache based on a user name included in the access control entry in Column 3, lines 49-65.

Referring to the rejection of claims 11 and 41, Etzel et al. discloses the claimed limitation wherein removing one mapping from the encrypted key cache while leaving one or more other mappings in the encrypted key cache in Column 8, lines 5-26.

Referring to the rejection of claim 12, Etzel et al. discloses the claimed limitation wherein removing the one mapping if the one mapping has not been accessed within a certain time frame in Column 4, lines 38-67, Column 5, lines 1-7.

Referring to the rejection of claim 13, Etzel et al. discloses the claimed limitation wherein removing the one mapping if the encrypted key cache is already full and a new mapping is to be saved in the encrypted key cache in Column 6, lines 23-42.

Referring to the rejection of claim 24, 28, 40, and 43, Etzel et al. discloses the claimed limitation wherein one or more computer-readable memories containing a computer program that is executable by a processor in Column 8, lines 62-67, Column 9, lines 1-39.

Art Unit: 2137

Referring to the rejection of claims 26 and 38, Etzel et al. discloses the claimed limitation wherein using the private key to decrypt the symmetric key corresponding to another file if the access control entry corresponding to the other file is not included in the encrypted key cache in Column 5, lines 8-65.

Referring to the rejection of claims 27 and 39, Etzel et al. discloses the claimed limitation wherein storing in the encrypted key cache, a mapping of the access control entry corresponding to the other file to the decrypted symmetric key in Column 5, lines 66-67, Column 6, lines 1-42.

Referring the rejection of claim 42, Etzel et al. discloses a method for accessing a key cache that maintains a plurality of access control entry to symmetric key mappings corresponding to a plurality of files accessible to a user in a distributed file system, wherein each of the plurality of files of mappings identifies a symmetric key that can be used to decrypt a file corresponding to the mapping, generating an encrypted file that includes a key cache and that is encrypted using a symmetric key, encrypting the symmetric key using a public key corresponding to the user, storing the encrypted symmetric key in an access control entry and storing the encrypted file and the access control entry corresponding to the encrypted file in the distributed file system in Column 3, lines 3-65 and Column 4, lines 9-34.

Referring the rejection of claim 44, Etzel et al. discloses a system for storing a plurality of access control entry to symmetric key mappings, retrieving an access control entry corresponding to a requested file, means for comparing the retrieved access control entry to the plurality of access control entry to symmetric key mappings for determining

Art Unit: 2137

whether any of the plurality of mappings match the retrieved access control entry and obtaining a symmetric key to be used to decrypt the requested file if one of the plurality of mappings matches the retrieved access control entry, decrypting the symmetric key, using a private key corresponding to the public key used to encrypt the symmetric key in Column 4, lines 35-67 and Column 5, lines 1-34.

Conclusion

3. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

Art Unit: 2137

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CDJ
cdf
July 8, 2005

Matthew Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137